RSAC 2025 Conference

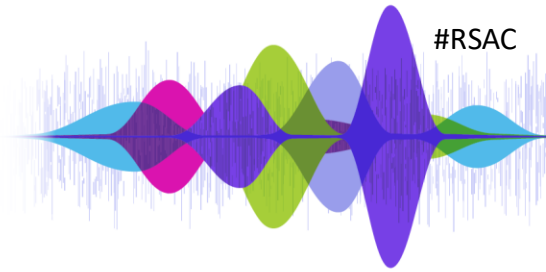
Many Voices.
One Community.

SESSION ID: BR-W02

SCION: Next-generation Inter-domain Networking Architecture

Jelte van Bommel

Research Scientist
ETH Zürich



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

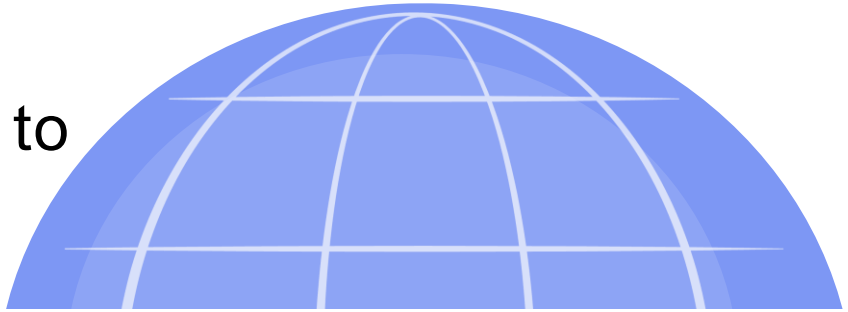
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Current Internet

Cyber attacks / interception
Data sovereignty breaches
Performance impact

Built on a **35 year old protocol** (Border Gateway Protocol, BGP), that was not intended to scale to billions of hosts



Sender has no control over the path their traffic takes over the internet

Catalin Cimpanu

February 14th, 2022

KlaySwap crypto users lose funds after BGP hijack

Feb 2022 - KLAYswap cryptocurrency hijack
Apr 2018 – Amazon Route 53 hijack
Feb 2008 – YouTube hijack

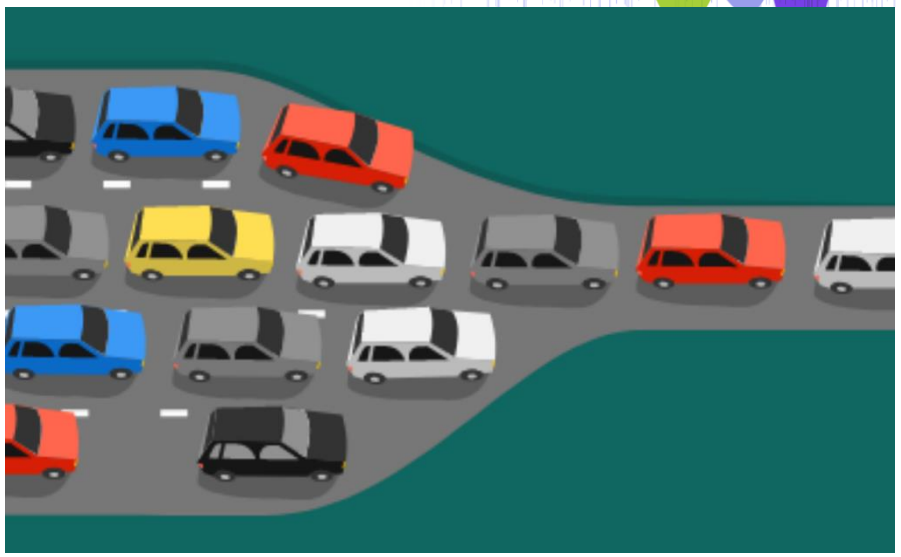
Current Internet is single path

- Routing protocol can switch route to traverse a link with limited capacity (bottleneck link)

  → High packet loss

- Since connectivity exists, often manual intervention needed to switch back to alternate path

- Frequent reason for outage, caused by misconfiguration or attack



How Verizon and a BGP Optimizer Knocked Large Parts of the Internet Offline Today

2019-06-24

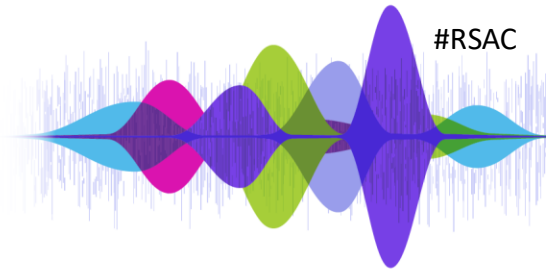
Tom Strickx

For two hours, a large chunk of European mobile traffic was rerouted through China

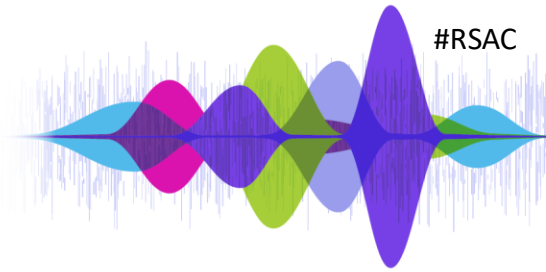
It was China Telecom, again. The same ISP accused last year of "hijacking the vital internet backbone of western countries."

Written by **Catalin Cimpanu,** Contributor

June 7, 2019 at 12:41 p.m. PT



How secure and reliable can a global internet be?



SCION™

Scalability, Control, and Isolation On Next-Generation Networks

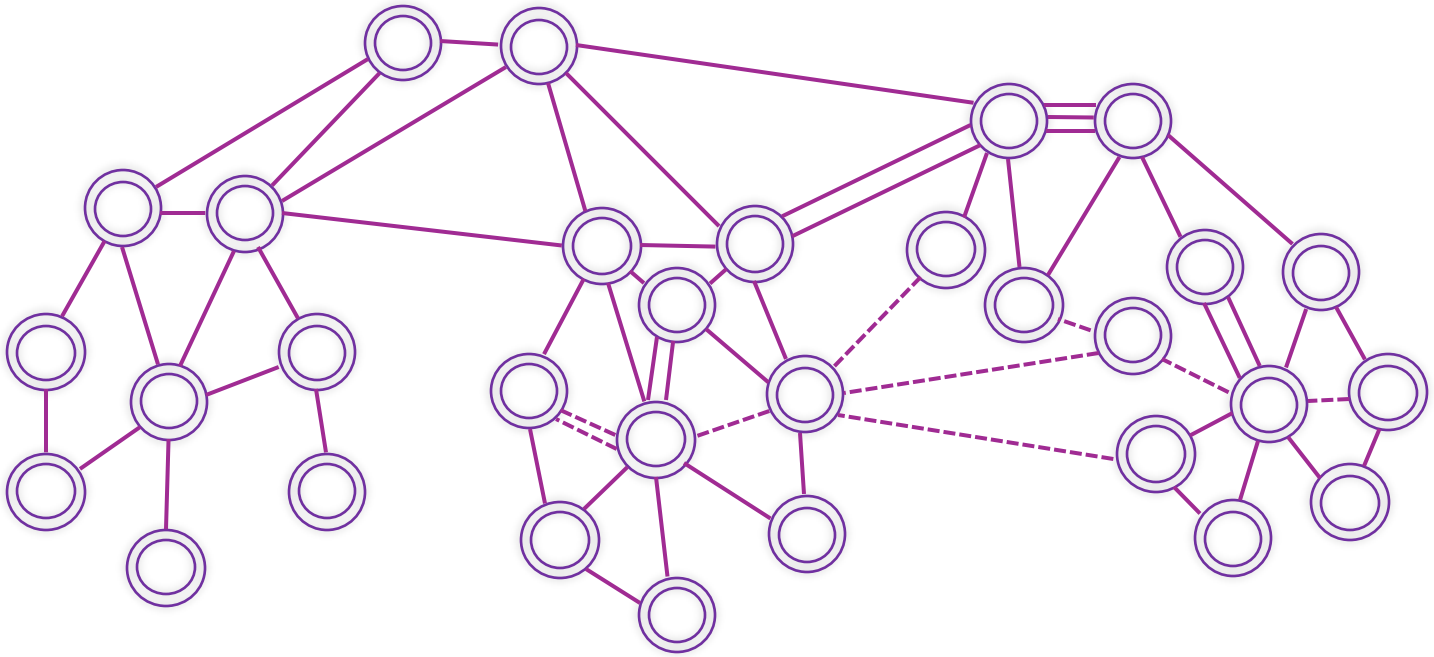
High security through design and formal verification

Path-Aware Networking

Multipath communication

Fault Isolation Domains

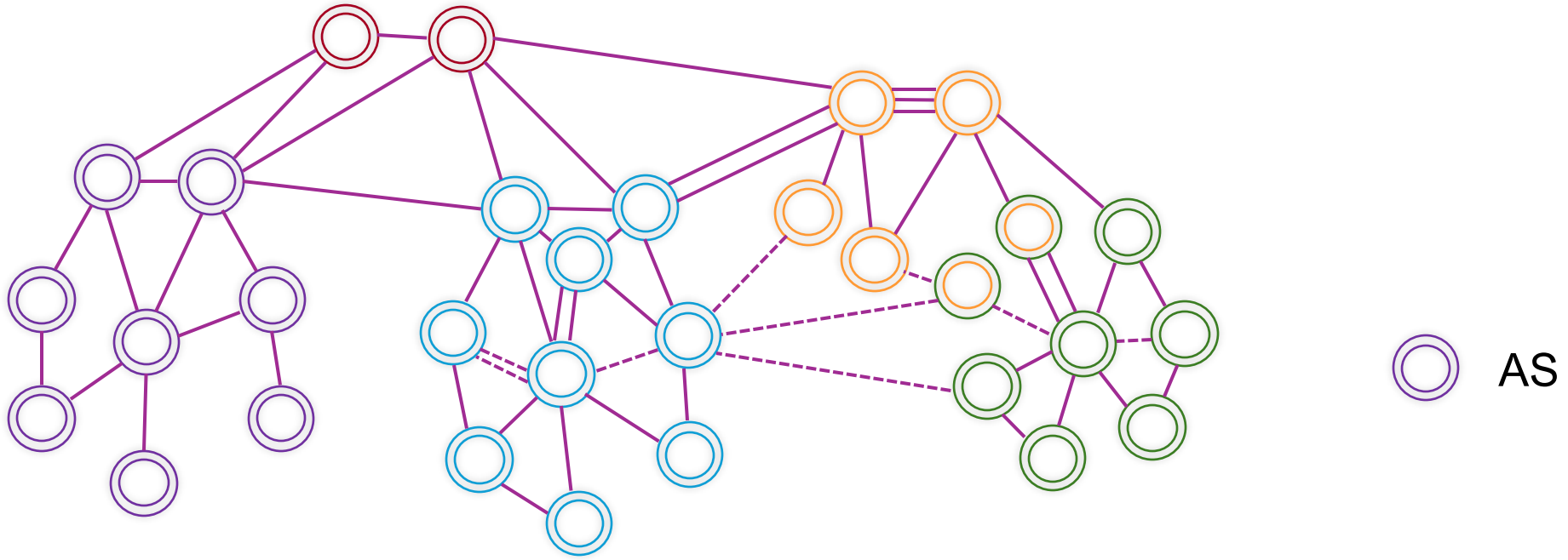
Rethinking the structure of the internet for scalability and security



Fault Isolation Domains

Rethinking the structure of the internet for scalability and security

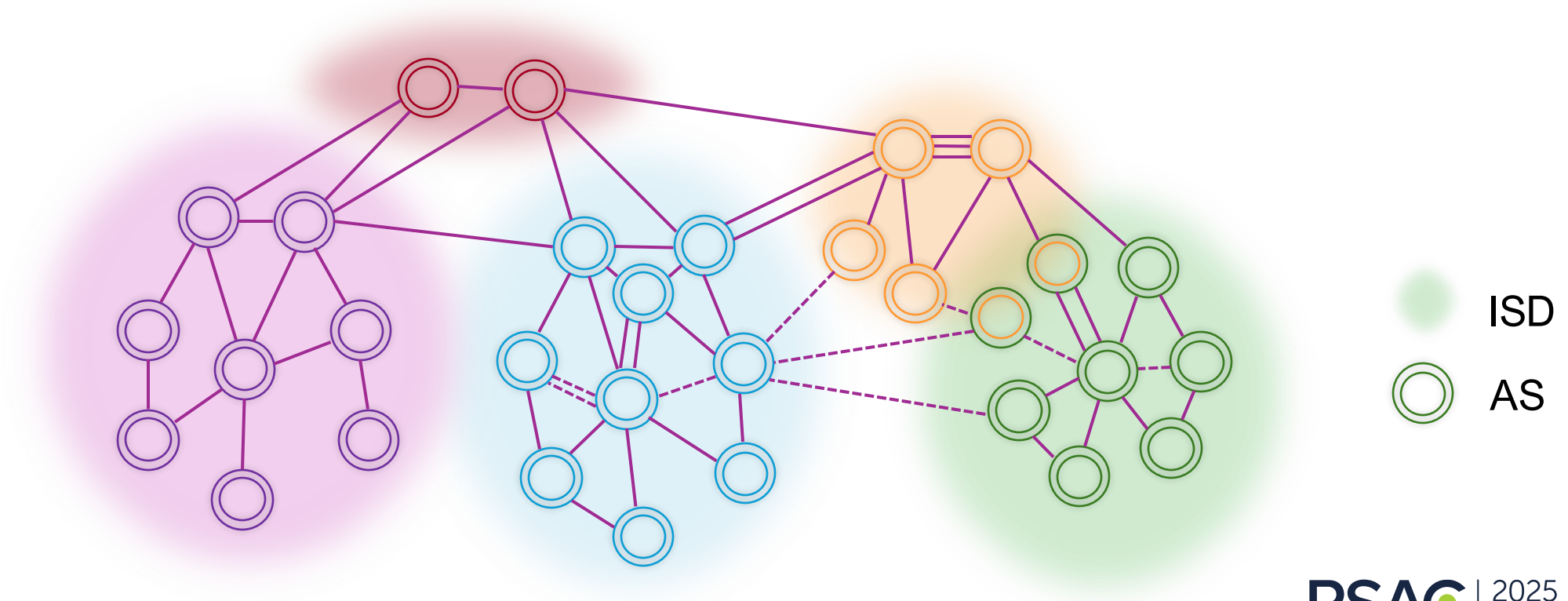
Logical grouping of uniform trust environment (e.g. a jurisdiction)



Fault Isolation Domains

Rethinking the structure of the internet for scalability and security

Logical grouping of uniform trust environment (e.g. a jurisdiction)



Fault Isolation Domains

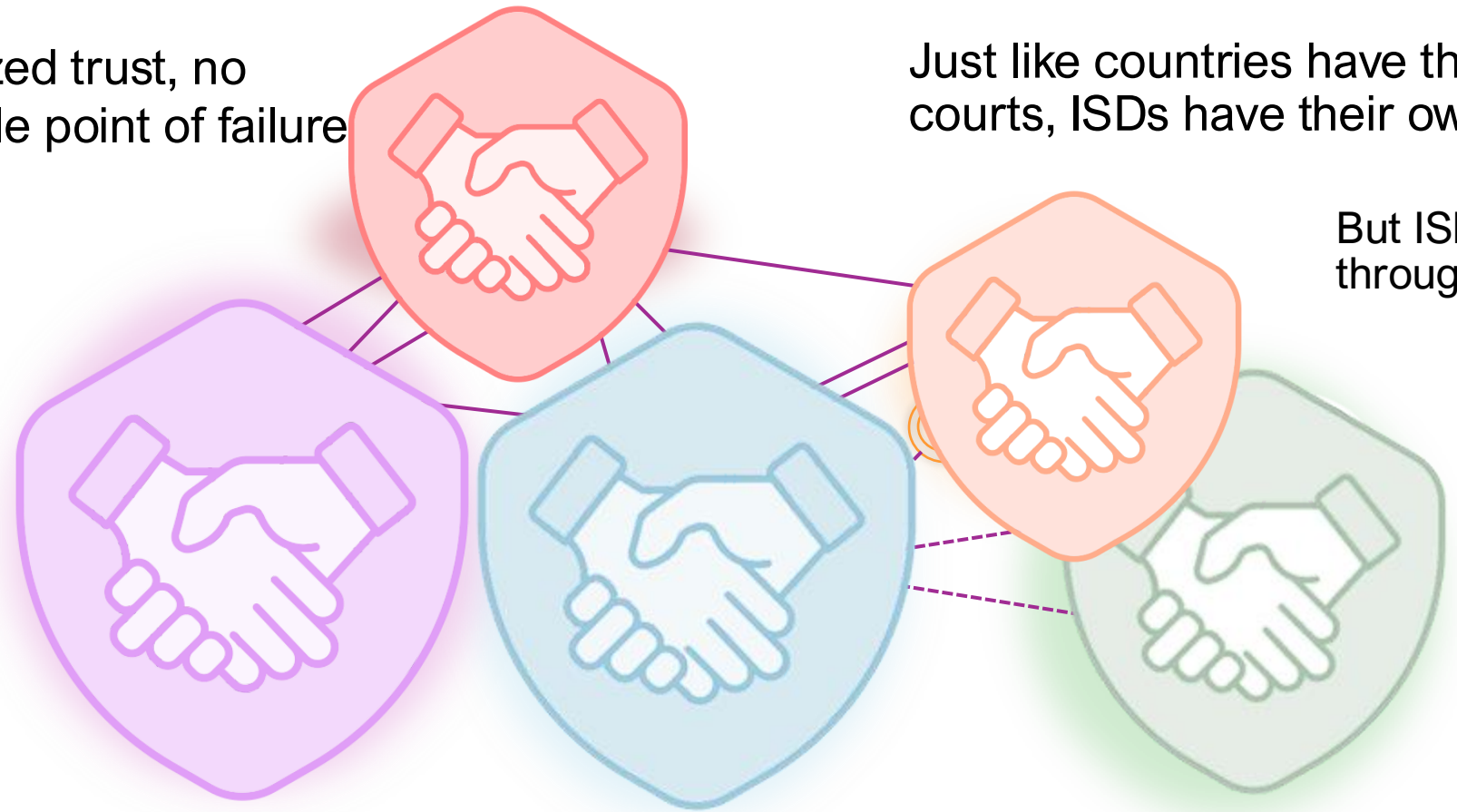
Rethinking the structure of the internet for scalability and security

Logical grouping of uniform trust environment (e.g. a jurisdiction)

Decentralized trust, no global single point of failure

Just like countries have their own laws and courts, ISDs have their own trust roots.

But ISDs can still interact through well-defined borders



Fault Isolation Domains

Rethinking the structure of the internet for scalability and security

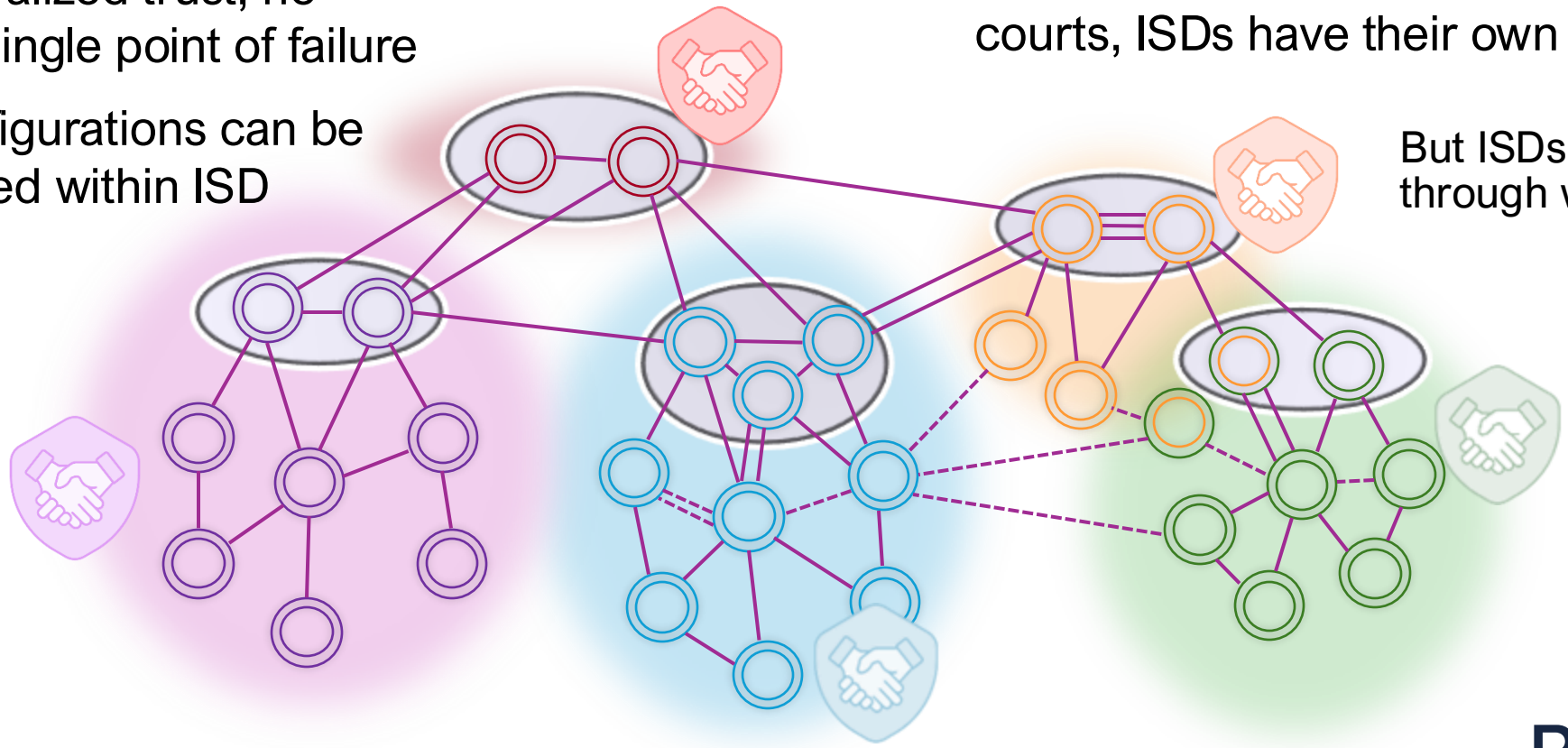
Logical grouping of uniform trust environment (e.g. a jurisdiction)

Decentralized trust, no global single point of failure

Misconfigurations can be contained within ISD

Just like countries have their own laws and courts, ISDs have their own trust roots.

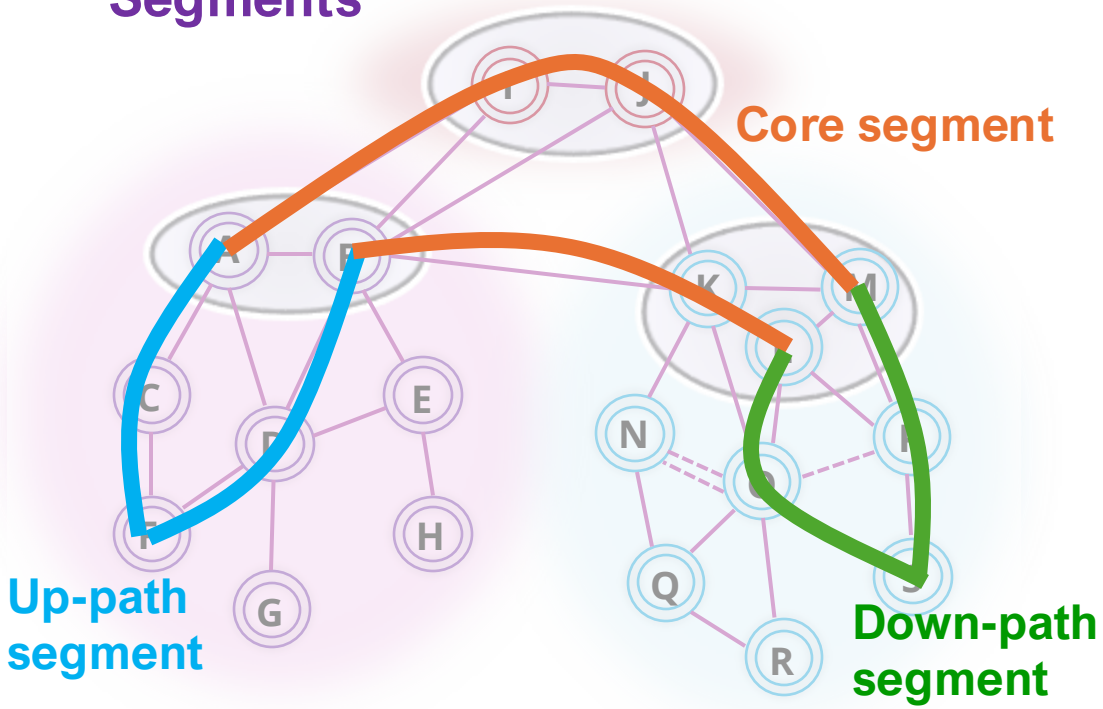
But ISDs can still interact through well-defined borders



SCION Architecture

Control Plane

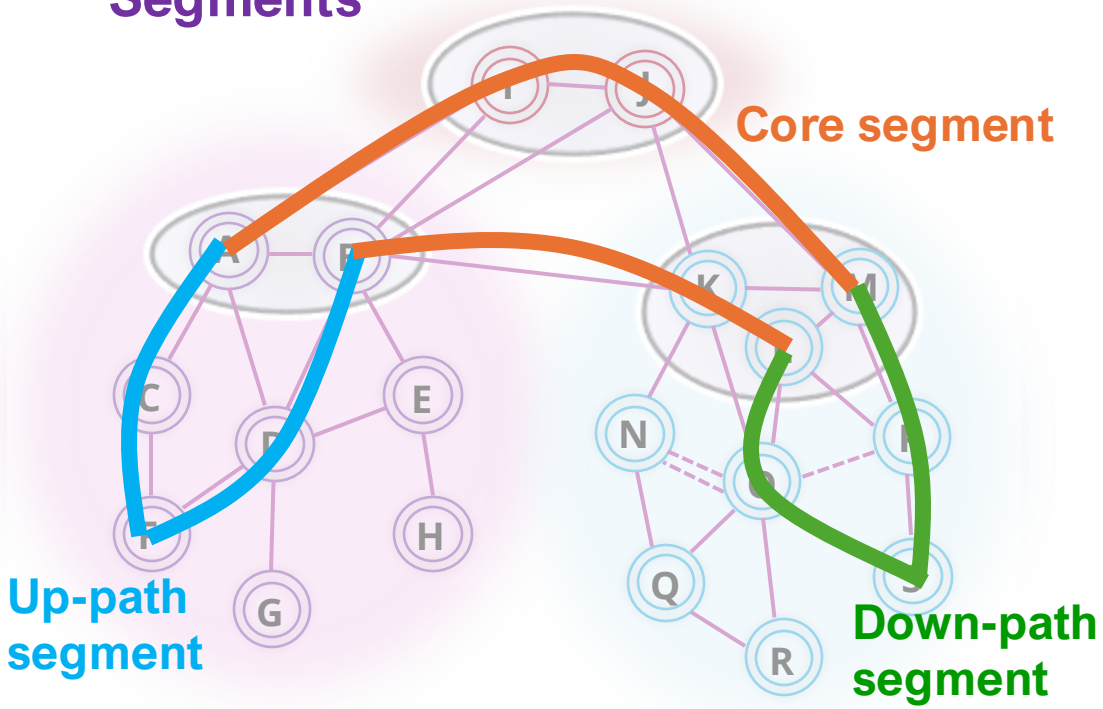
Constructs and disseminates **Path Segments**



SCION Architecture

Control Plane

Constructs and disseminates **Path Segments**



ASes add metadata to path segments, such as latency or bandwidth info

Data Plane

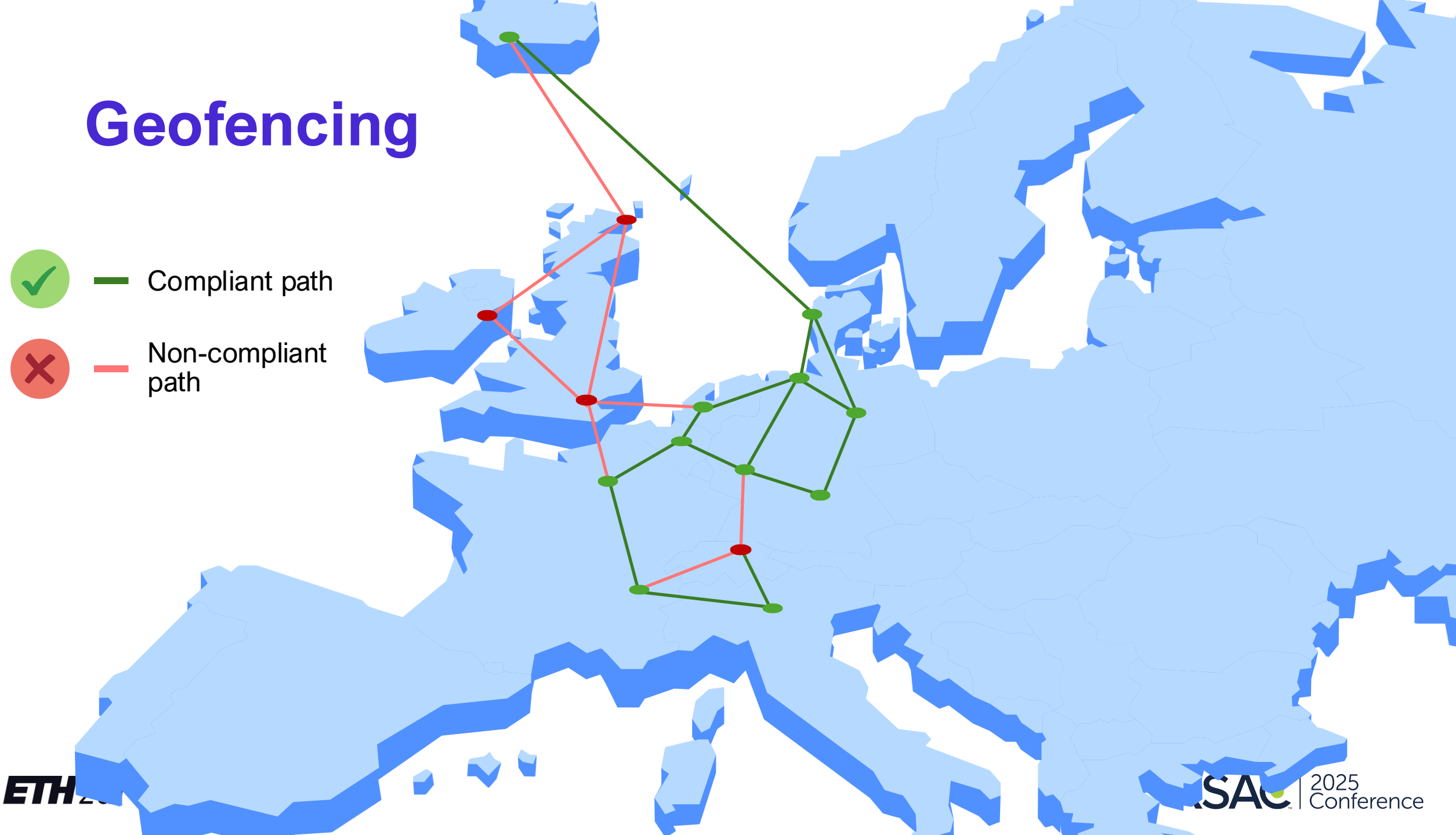
Sender combines **Path Segments** to **Path**

Sender can optimize path for specific requirements, e.g. based on metadata.

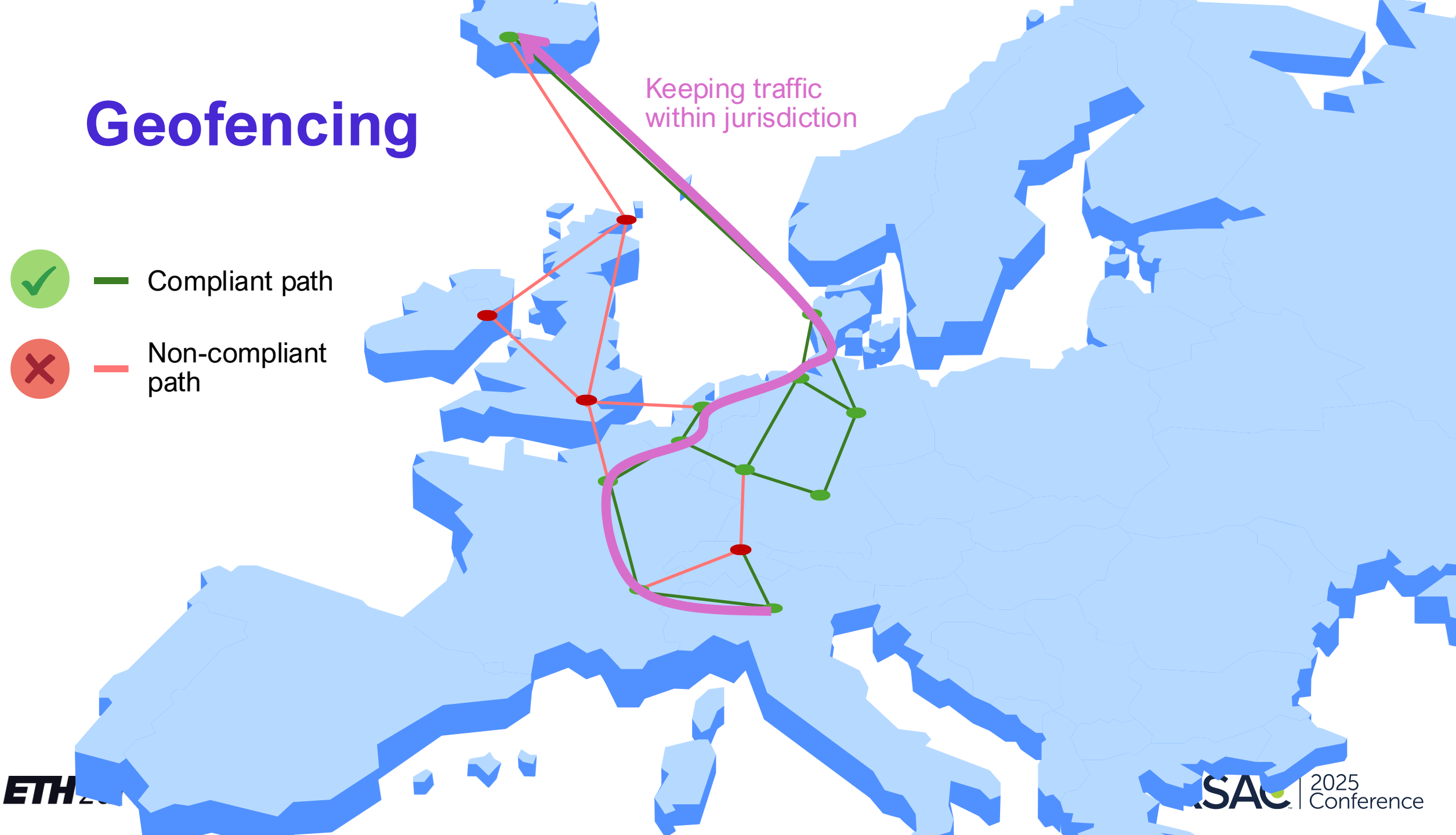
Stateless routers forward packets based on **Path** in packet header

Geofencing

Geofencing



Geofencing


Keeping traffic
within jurisdiction
Compliant path
Non-compliant
path

Resilience

South China Morning Post

China unveils a powerful deep-sea cable cutter that could reset the world order

Beijing now has the power to disrupt global communications after scientists revealed a device that can sever undersea cables

Resilience

Fast-path failover

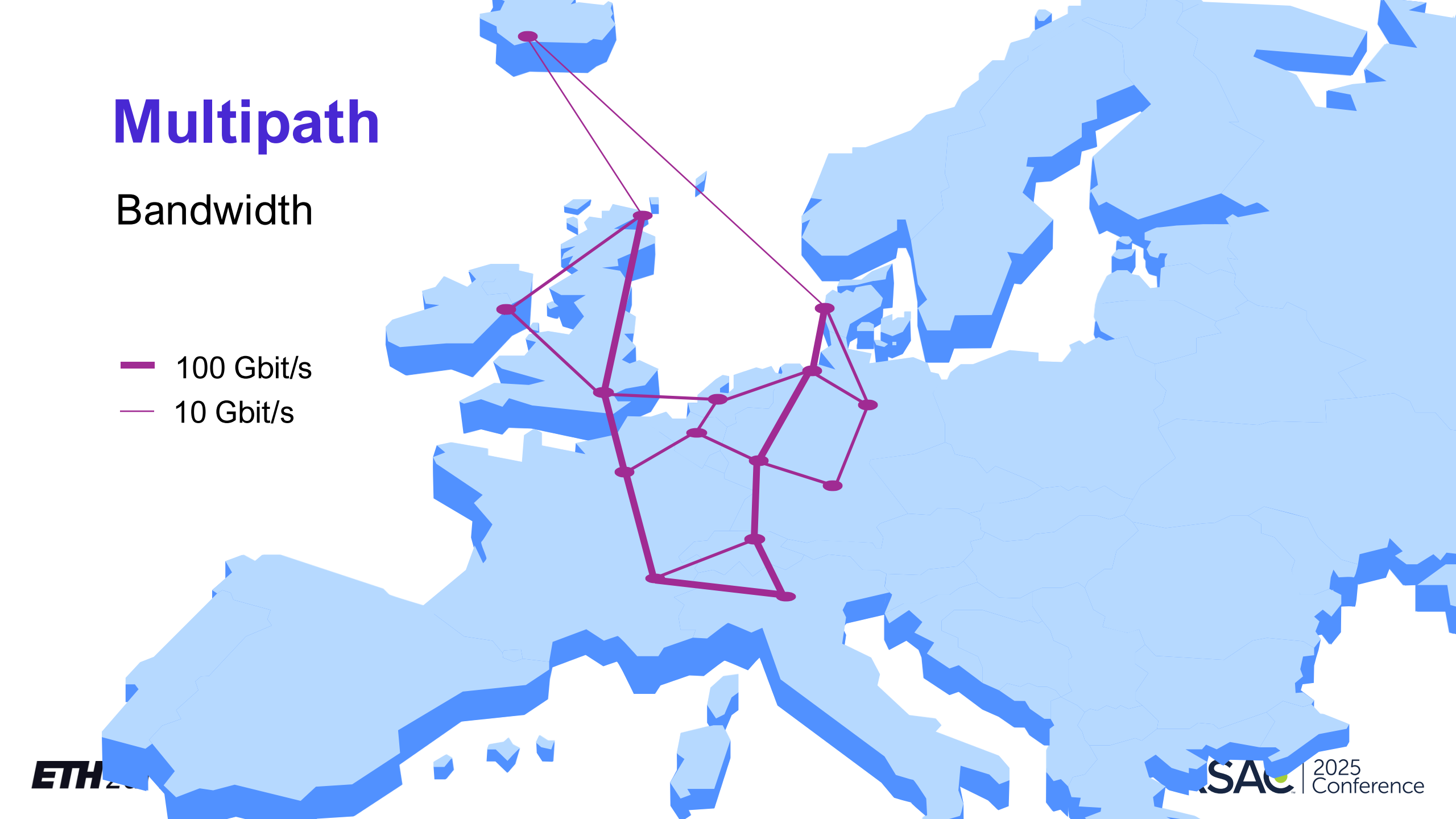
South China Morning Post

China unveils a powerful deep-sea cable cutter that could reset the world order

Beijing now has the power to disrupt global communications after scientists revealed a device that can sever undersea cables

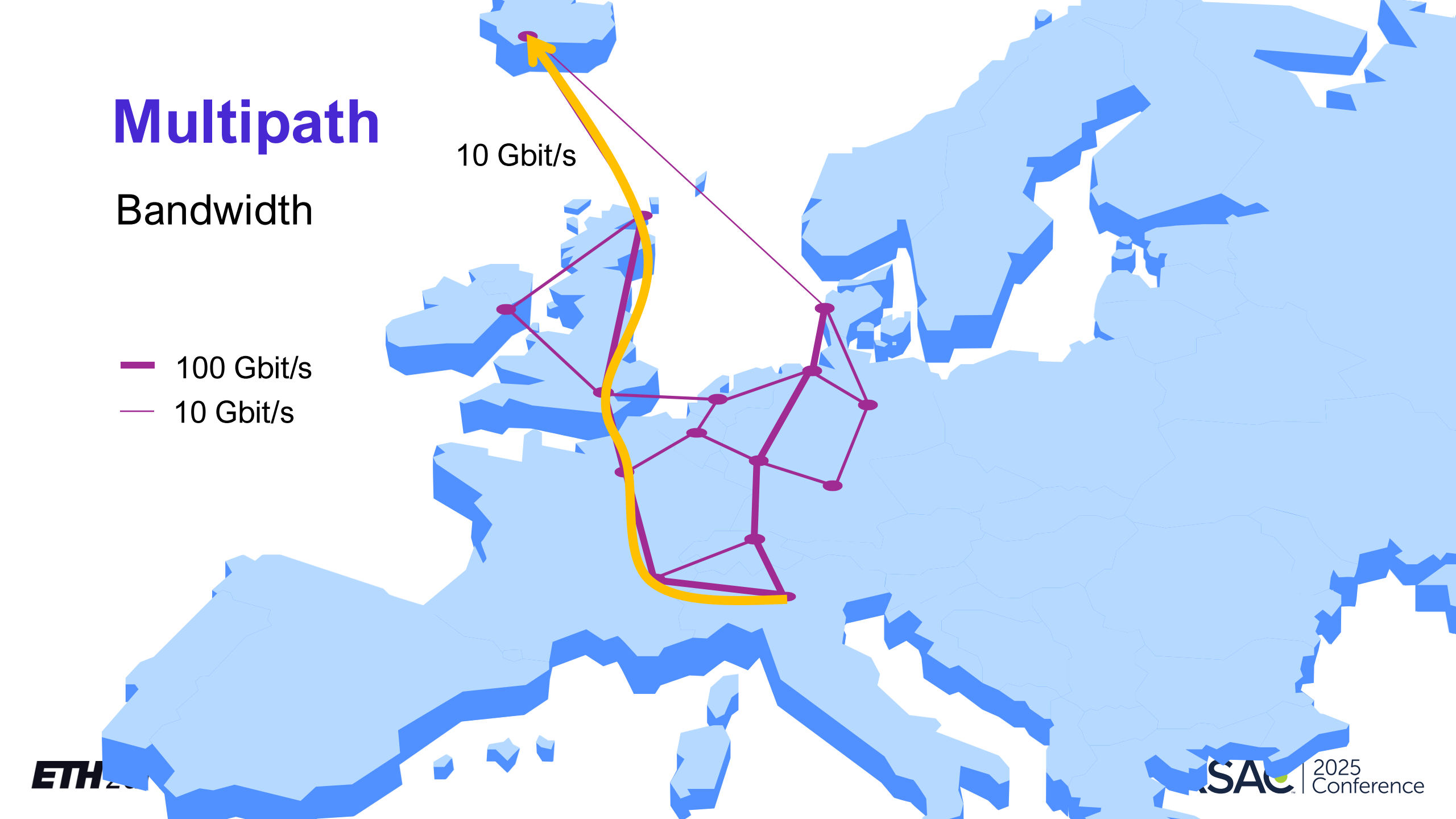
Multipath

Bandwidth



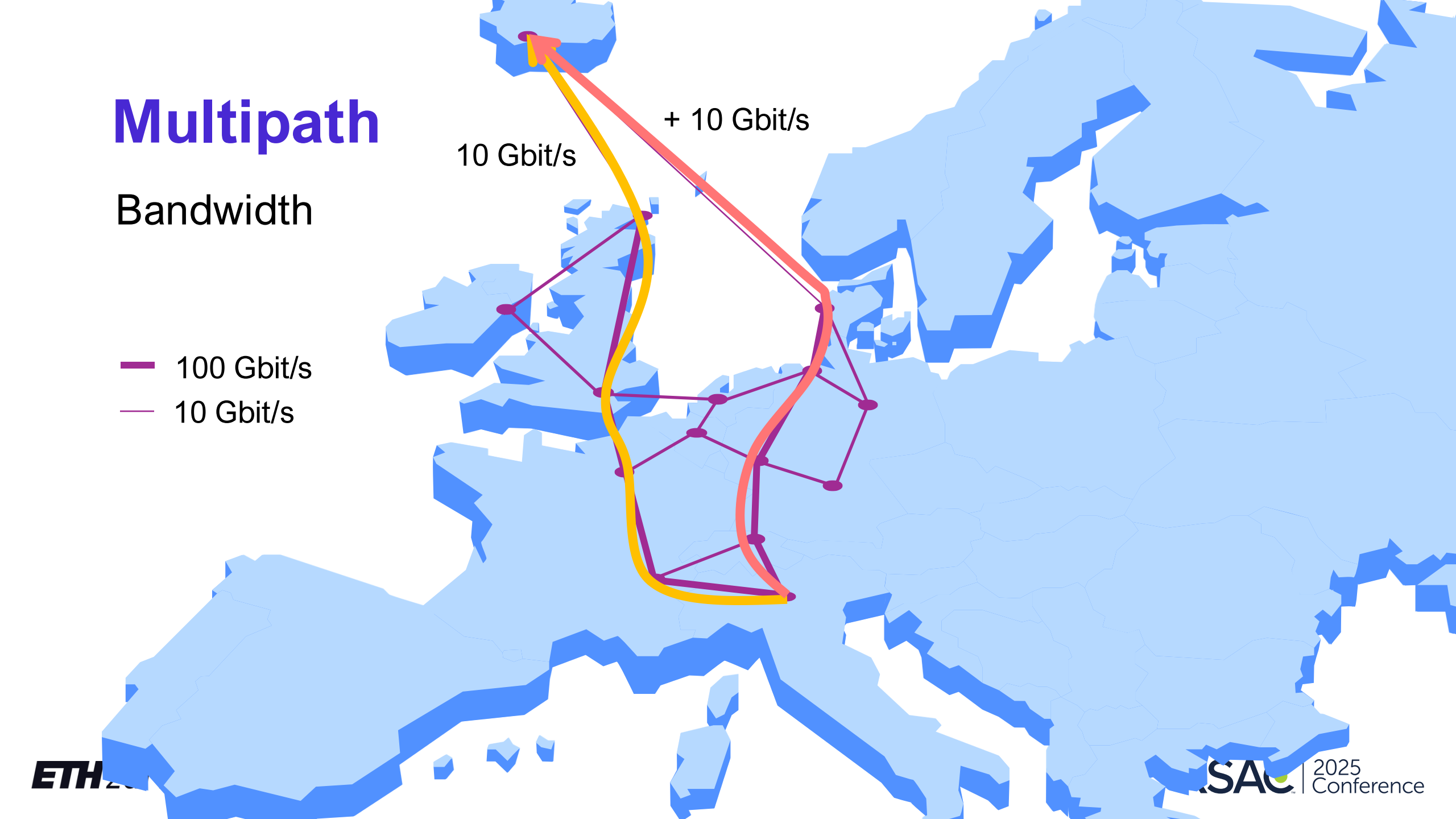
Multipath

Bandwidth



Multipath

Bandwidth



Importance of Path Awareness & Multipath

Generally, two paths exist between Europe and Southwest Asia

- High latency, high bandwidth: Western route through US, ~450ms RTT
- Low latency, low bandwidth: Eastern route through Suez canal,~250ms RTT

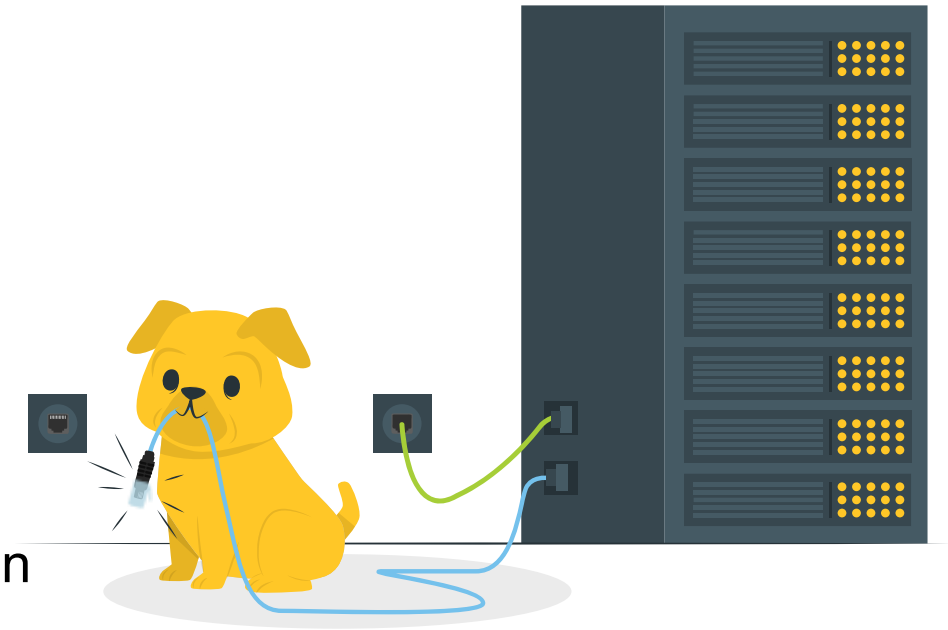
BGP typically “money routing”, **offers cheapest path.**

Depending on application, **either path** is preferred.

With SCION, both paths can be offered!

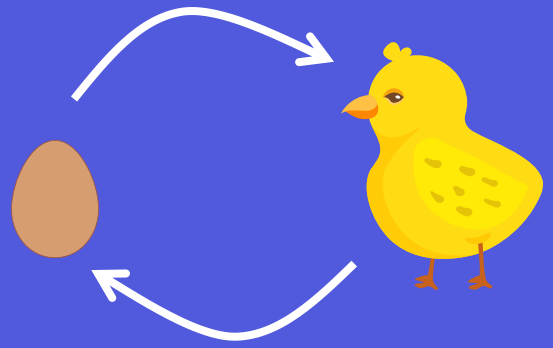
Multipath is a necessity for high availability and performance

- Rapid failover without routing system convergence
  - Routing bottlenecks can be avoided
- Enable higher network capacity
  - No more passive links for redundancy, all links can be active
  - Simultaneous use of several links
- Enables higher communication efficiency
  - Latency- vs. bandwidth optimal paths can be chosen
- Helps defend against DoS attacks, as adversary needs to congest all links



This seems impossible to deploy!

Need early adopters deploying the architecture



Need initial deployment to convince early adopters

How to Deploy SCION:
Operate alongside today's internet

- SCION reuses the existing infrastructure
  - SCION leverages UDP+IP as a local "Layer 2.5" underlay
  - **No change** to the internal network infrastructure needed
- Endpoints can **either**
  - run a SCION stack or
  - use SCION IP Gateways

No upgrades of end hosts or applications needed

- SCION provides a communication fabric that is **independent of the existing BGP-based infrastructure**
- **Can see it as a second connection offering with more features, security and redundancy**

How to Deploy SCION:
Communication among Community

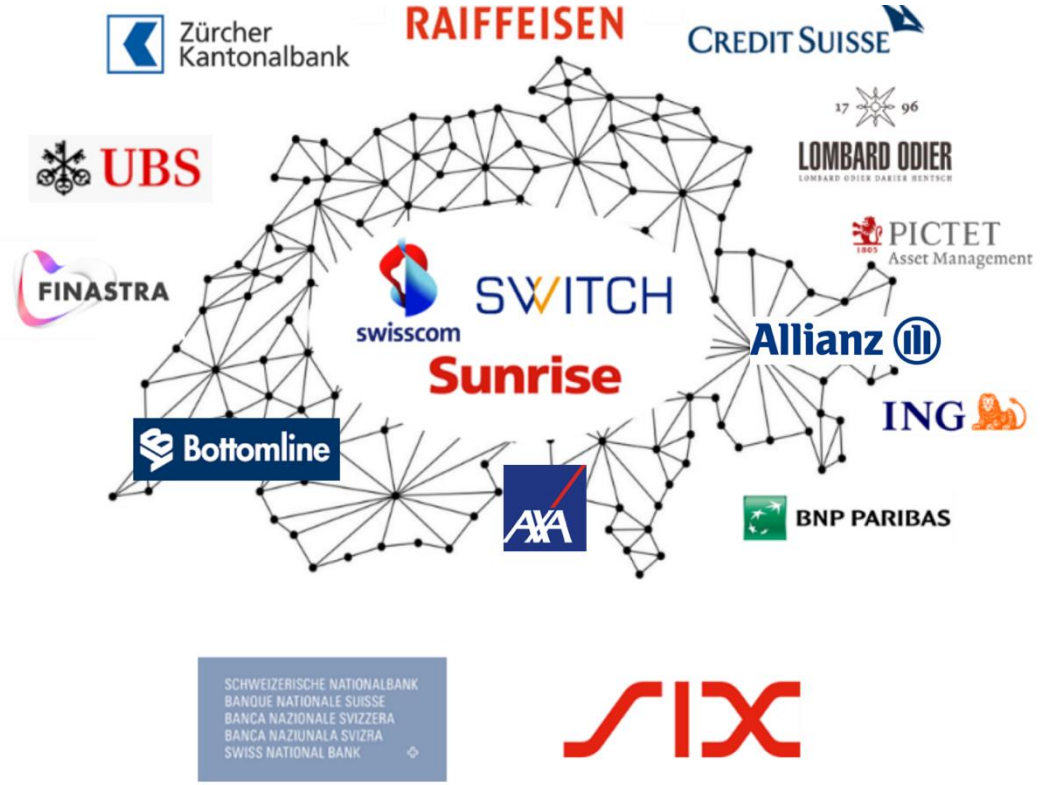
Single SCION connection offers secure communication to any other entity on SCION network

A single SCION connection approximates a leased line to all SCION destinations

SCION Deployment:
Secure Swiss Finance Network (SSFN)

Swiss inter-banking network handling money transfers between banks and other critical real-time financial services

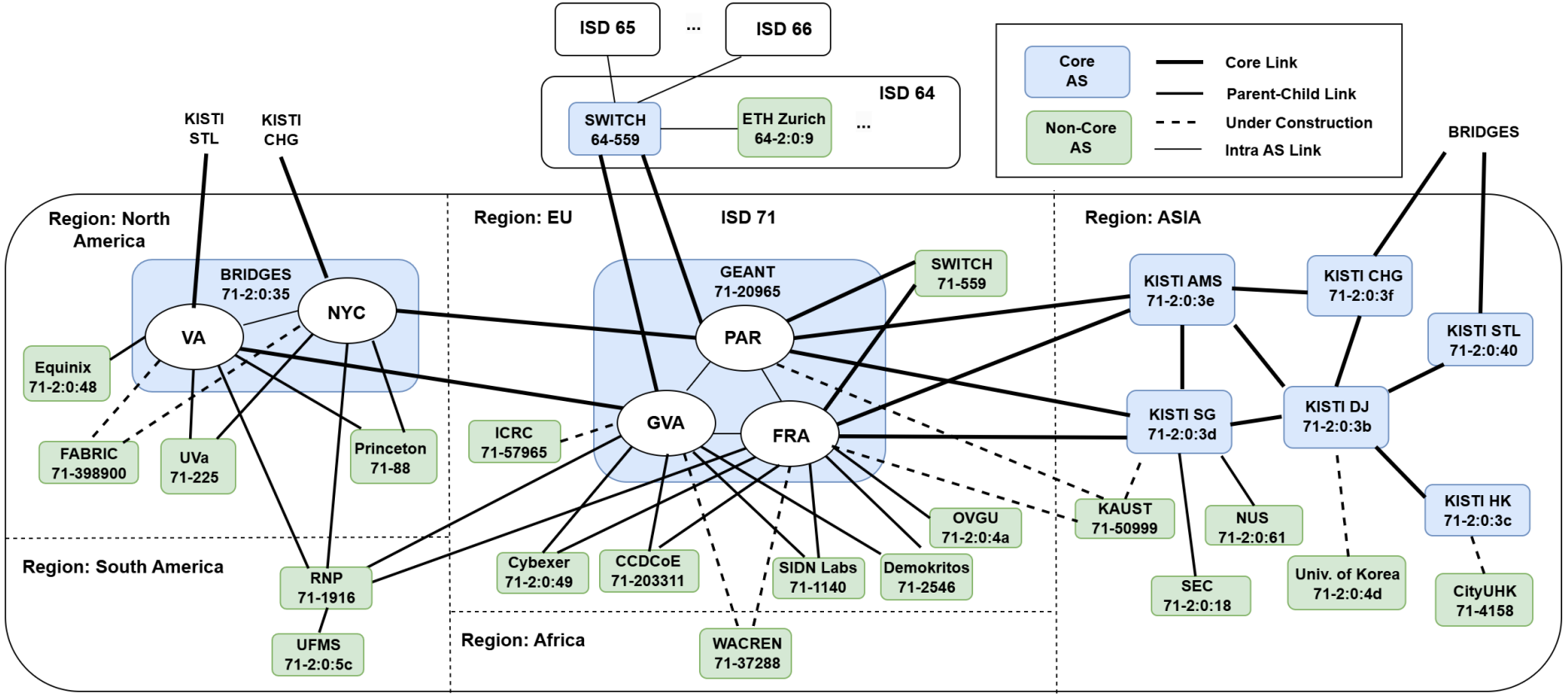
- 321 participants, including 280 banks, 14 insurance companies and 12 securities firms
- 2.9 million transactions, representing 178 billion CHF (~202 billion USD) per day
- New secure, reliable, community-based and sovereign network announced in July 2021



Logos are illustrative

SCION Deployment:
SCION Education, Research and Academic Network (SCIERA)

Native SCION connectivity for 250’000+ users



Growing SCION Ecosystem

Any ISP can connect to the SCION internet and provide new connection offerings → new opportunities to generate revenue

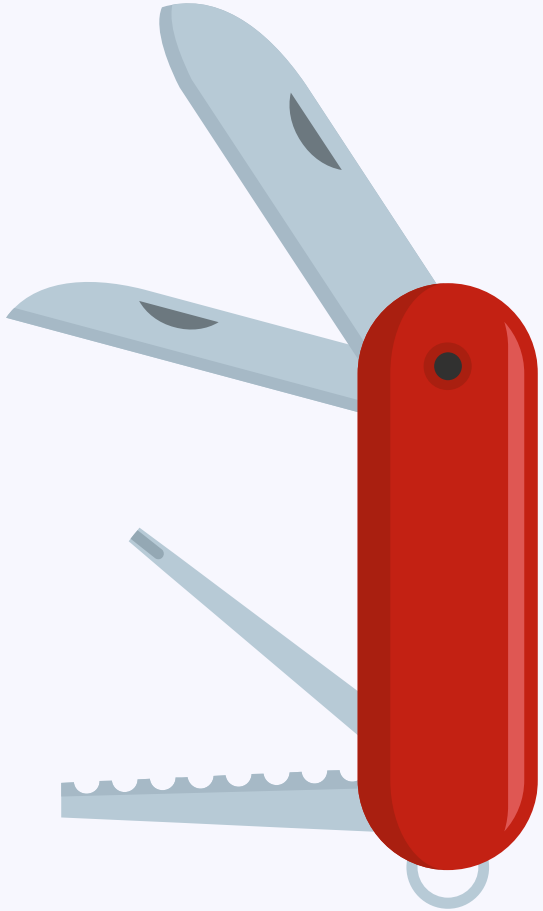
That’s not all…

1 **SCION facilitates efficient source authentication**

Fundamental defense against source address spoofing (often utilized in DDoS attacks)

2 **SCION enables bandwidth reservation schemes**

Guarantee bandwidth to users or critical applications and reduce congestion



RSAC 2025 Conference

Many Voices.
One Community.

Use SCION today

- Read “The Complete Guide to SCION” book
- Set up a SCION AS and experiment
  - scionlab.org
- Try SCION applications
  - scion-architecture.net/apps
- Build on SCION
  - github.com/scionproto/scion

Thank You!

Contact us at

netsec.ethz.ch

Jelte van Bommel

Network Security Group

ETH zürich

To achieve strong assurances for a large-scale distributed system, **formal security verification is necessary**

VerifiedSCION

- Performing formal verification from the beginning avoids “difficult-to-verify” components
- Many design aspects of SCION facilitate formal verification
- An aspect is ensuring there are no circular dependencies

PCB Contents

Creation time

Base information

AS Name: M

Hop Field

Link Identifiers:
0,1

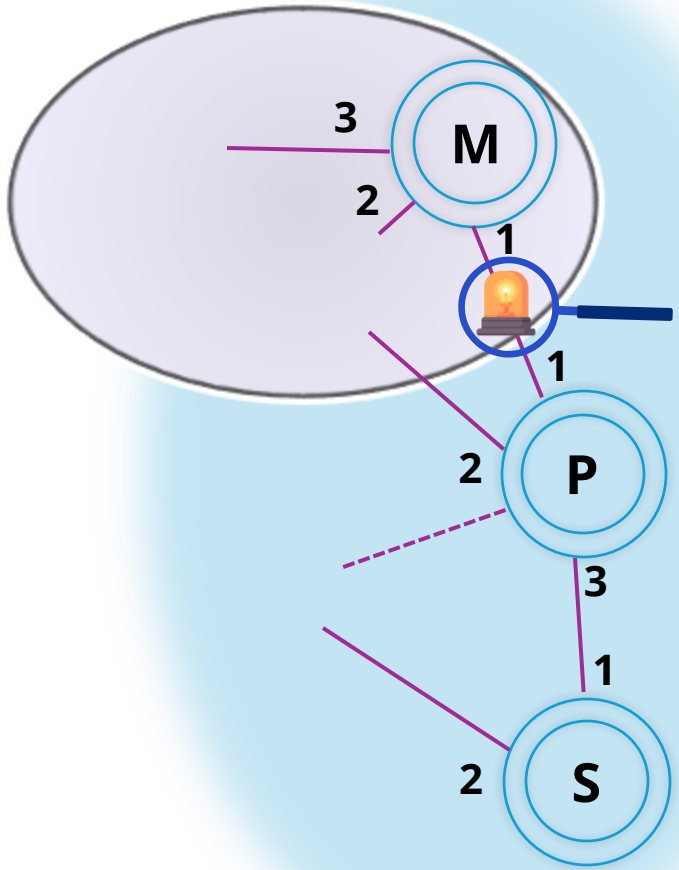
Expiration Time:
In 6 hours

MAC

AS Entry

Metadata:

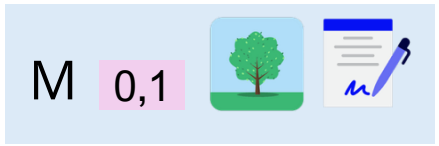
AS signature:

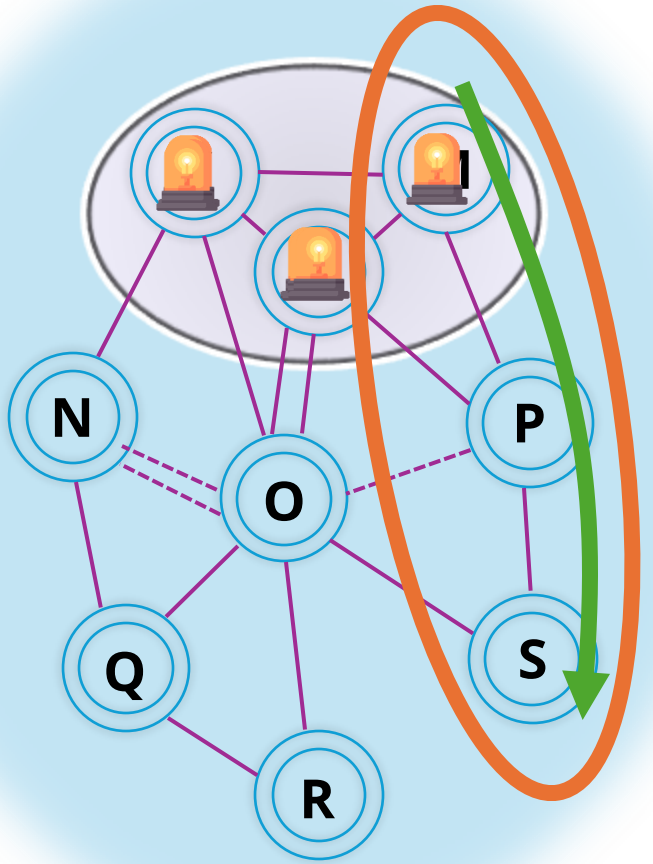


Control Plane

Beaconing

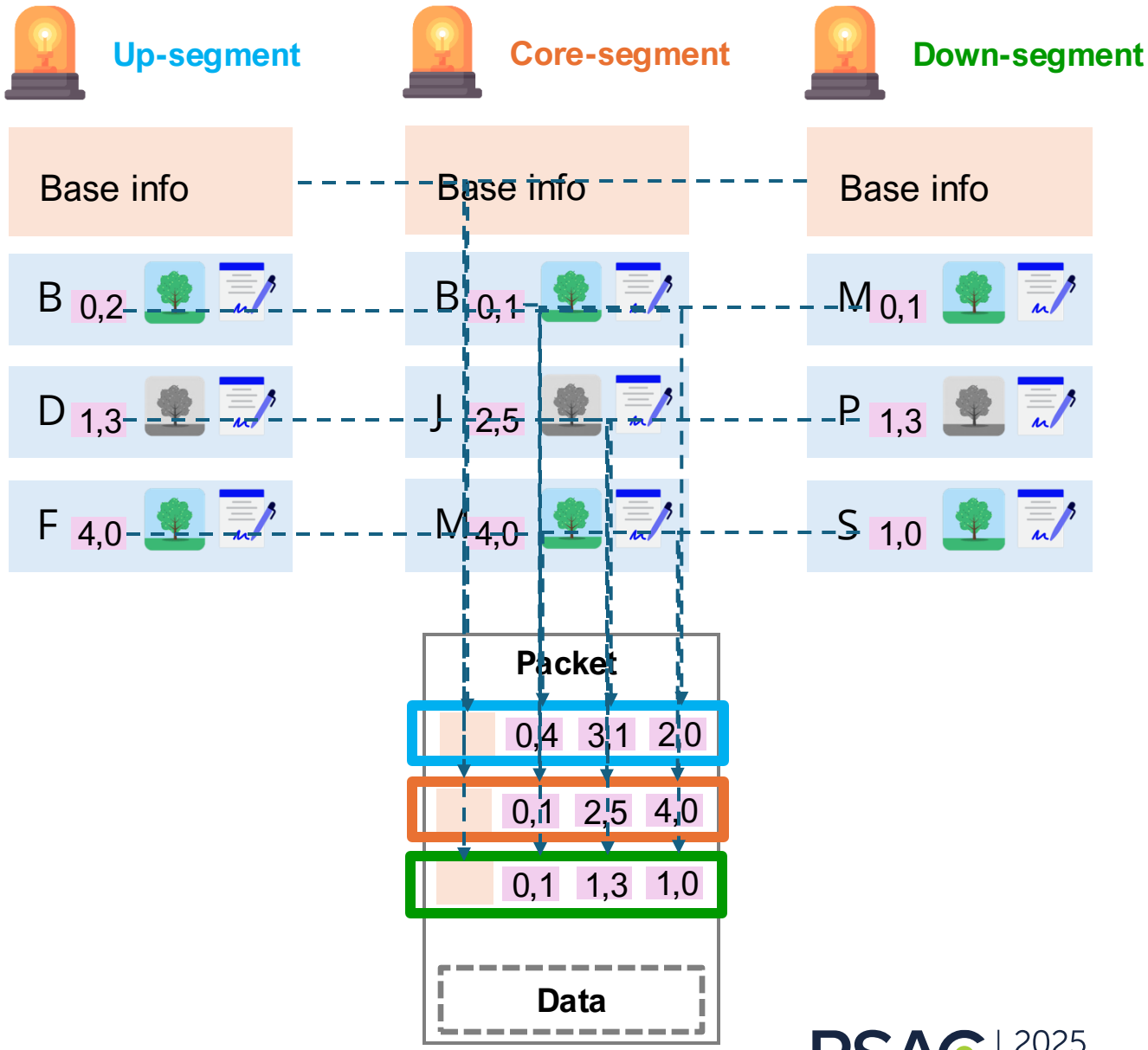
- Core ASes initiate **Path-segment Construction Beacons** (**PCBs**), or “beacons”
- PCBs traverse ISD as a flood to reach downstream Ases
- PCBs collect information as they traverse the network





Data Plane

- **Path** is encoded in the packet header
- Routers forward packets based on **Path**
- (Stateless) routers only verify the authenticity of the information
  → two AES cryptographic operations replace (expensive) longest-prefix match in BGP



Segment Registration

Up-path segment:

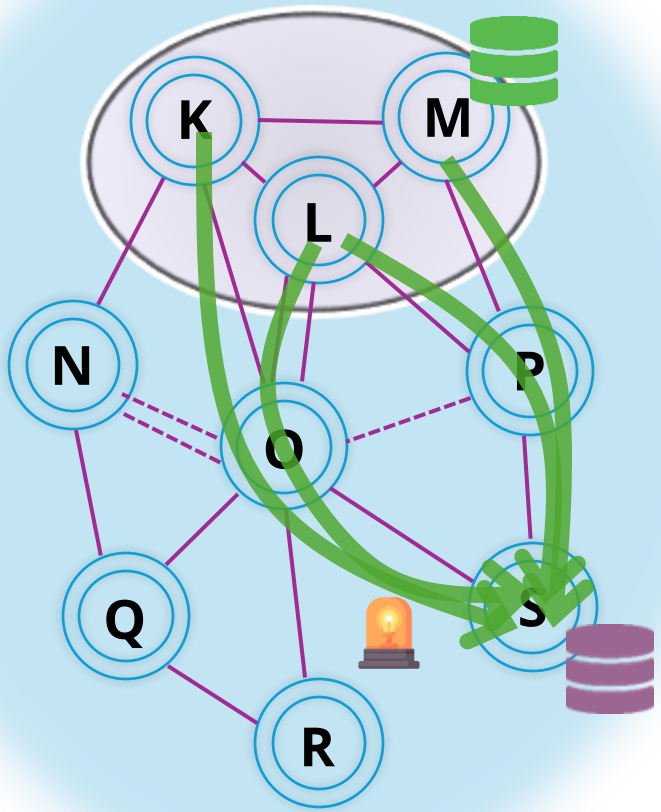
from AS to core AS (S → L)

- **Up-path** segments are registered at **local path servers** (in S)

Down-path segment:

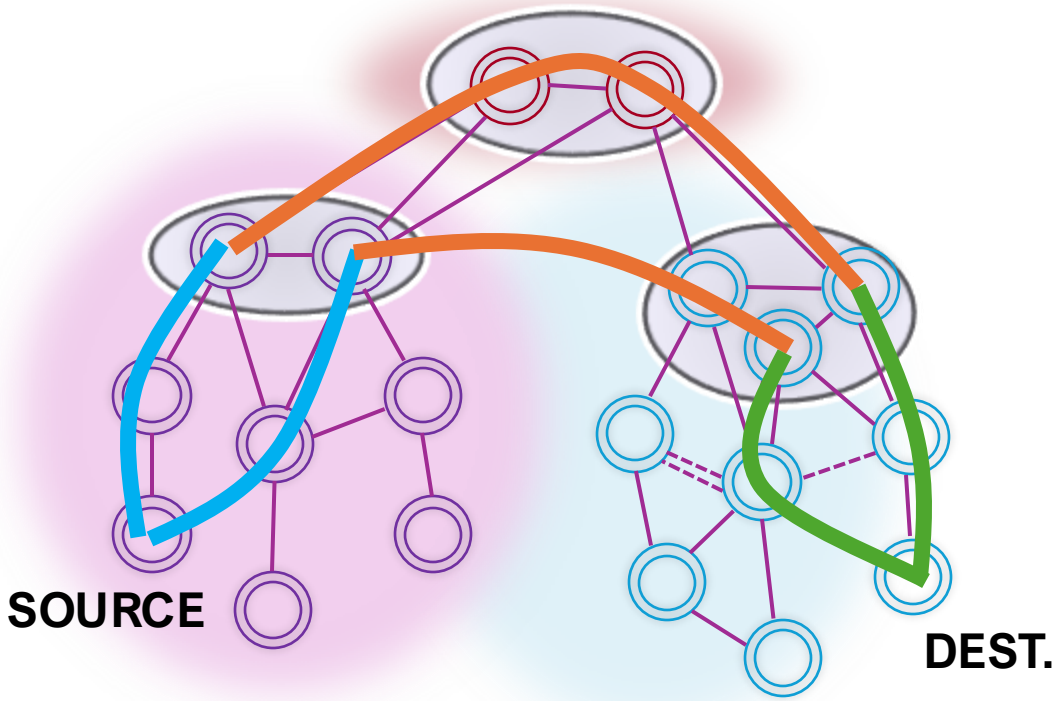
from core AS to AS (L → S)

- **Down-path segments** are uploaded to **core path server** in **core AS**



Putting it all together:
Communication to Remote ISD

- Host contacts local path server requesting **<ISD,AS>**
- If path segments are not cached, local path server will contact core path server
- If core path server does not have path segments cached, it will contact remote core path server
- Finally, host receives up-core, and down-segments



Observation: Scalable Path Discovery and Dissemination for Rapid Global Connectivity

- Reasons for scalability
  - AS-level instead of IP prefix based routing
  - Leaf ASes only receive but do not forward any beacons (only core ASes initiate beacons)
  - Beaconing does not require iterative convergence
- Consequences
  - Rapid path exploration between all pairs of core ASes
  - Near “instantaneous” path exploration within ISD
  - Simulations suggest that global connectivity after “Internet cold boot” is achieved within seconds